INeS™ Certificate Lifecycle Management

Scalable platform for managing IoT devices Identities & Security enabling secure access to IoT data

SERVICES

• **High volume X.509 certificates** to create unique identities for millions of devices.

• **Managed PKI Services** to create and manage Root CAs, Subordinate CAs, and end-entity certificates (and key pairs) for the entire ecosystem *while* ensuring security and business continuity for the end-to-end lifecycle.

• **We provide the solutions** for secure access control, mutual authentication to establish point-to-point TLS communications, secure over-the-air updates and data protection and privacy.

• **Custom PKI Services** – we work with you to develop PKI services that meet your business needs.

The biggest barrier to deploying IoT projects is providing robust security that can be scaled for a large number of devices. The core security challenges are device personalization and lifecycle management. Devices need to be provisioned with unique, trusted identities that can interact in complex ecosystems of industrial and consumer IoT only with trusted entities.

WISekey Public Key Infrastructure (PKI) service called INeS provides device personalization at the massive scale you need to launch your project and manage your risk effectively. Whether you want to deliver credentials on the factory floor or from an online cloud-enabled service (like AWS IoT, Azure IoT & GCP IoT), WISekey makes scalable device personalization easy.

Focus on Your Core Business
Running a certificate management operation requires specialized facilities, processes, technology and skills. WISekey has the expertise to run your operations, allowing you to focus on your core business. Our world class operation delivers the most scalable and secure PKI services in the industry. WISekey certificates are compliant with protocols like ***Wi-SUN*** (wi-sun.org) or ***OPC*** (opcfoundation.org) or ***ISO 15118*** plug & charge for EV

Use Cases

INDUSTRIAL IOT MEDICAL IOT
WISekey provides unique identities for each device, application, service, and user to secure operations

SMART CITY
WISekey can help maintain the end-to-end integrity of smart infrastructure for cities

CONNECTED CARS
WISekey delivers trusted identities to components within a car to secure end-to-end communications

MANAGED PKI SERVICES

• **Root CA Flexibility –** You have the option to let us create and manage a Root Certificate Authority (CA) specifically for you, or to use a Publicly Trusted WISekey Root CA.

• **Bulk X.509 Certificates –** We can deliver X.509 certificates in batches of any size from hundreds to millions, along with their corresponding private keys to satisfy any scale of project.

• **Revocation –** We manage certificate revocation lists, OCSP, and other revocation mechanisms if private keys become compromised.

• **Storage and Backup –** WISekey manages your root keys in secure facilities and HSMs, backed up across multiple physical locations to ensure business continuity.

• **Secure Service –** WISekey provides you secure access to the Service through Web portal and REST API enabling automation

• **Test and Production Environments –** Allow development and test activities to proceed without affecting production operations.

CUSTOM PKI SERVICES

• **Ecosystem PKI Design.** We can design the PKI hierarchy for your entire implementation, including Root CA, Subordinate CAs, services, devices, applications, platform providers, OEMs and whatever else you need.

• **Easy to Manage PKI**. Back-end services are provided through a battle-tested and fully audited web portal for ordering, deploying, revoking and managing credentials. The Service is provided As-a-Service or on-premise.

HIGH VOLUME PROVISIONING

• **Offline Provisioning.** We deliver batches of customized X.509 certificates for you to provision on your **factory floor** or in your own online field provisioning system.

• **Online Provisioning.** Provision identities to devices by getting credentials from a Wisekey hosted secure, multi-tenant, cloud-based repository at **initialization time (device onboarding)**.

STANDARDS COMPLIANCE

• **WebTrust Compliant and ISO 9001:2015 certified –** Wisekey defends against insider or intruder attacks via secure facilities, processes and technologies, including HSMs and having in place tested business continuity capabilities. A robust Quality System ensures ongoing process quality and continual improvement.

• **Auditable Reporting –** All operations are logged, and actionable reports are created to help meet compliance and regulatory requirements.

• **Cryptographic Standards & Protocols –** RSA 1024/2048 bit, Elliptic Curves (X9.62 curves, SEC curves, NIST curves, Teletrust curves), AES 128/192/256-bit, x.509 v3, RFC 5280, RFC 4325, RFC 2560, FIPS 140-2, PKCS #7, #8, #10, #12.

Learn more at wisekey.com

sales@wisekey.com